Security Awareness in Virtual Communities: The Case of Non-collocated Academic Research Collaborations

Adam Marks, Yacine Rezgui

Security Awareness in Virtual Communities: The Case of Non-collocated Academic Research Collaborations

Adam Marks[1] and Yacine Rezgui[2]
[1]Department of Business Administration, World Wide
Embry-Riddle Aeronautical University,
Marksa@erau.edu
[2]School of Engineering, Cardiff University, Queen's Buildings,
The Parade, Cardiff CF24 3AA, Wales, UK,
RezguiY@cardiff.ac.uk

Abstract. Internationalization of research is reflected in the distributed nature of research communities. Research has a strong collaborative dimension. It is often carried out by non-collocated individuals and teams in the context of national / international funded programs, institutionally led projects, or simply self-motivated initiatives. Universities form a strong and influential component of these virtual research communities. Advances in information and communication technologies (ICT), including the Internet, have helped sustain these virtual research communities. However, despite the strategic nature of research, there exist various levels of awareness about the security risk factor linked with virtual collaboration. This study examines the security awareness of academics and researchers across higher education institutions with a focus on three different academic settings. The paper suggests that a security awareness program aimed at academics should be initiated across universities to pave the way to security aware research collaborative communities.

Keywords: Virtual Collaboration, Research Community, Security Awareness

1 Introduction

Universities are among the least Information Systems (IS) secured environments [2]. Only a fraction of universities provide security and conduct awareness training [15]. Colleges and universities are targeted for cyber attacks for two main reasons; first, is the vast amount of computing power they posses; and second, is the open access they provide to their constituents [9]. In addition, universities have a considerable amount of confidential and strategic information that makes them prone to IS security threats [11]. Most IS managers tend to focus more on technical security solutions such as firewalls, routers, and intrusion detection software; but much less on hazards caused by end users' lack of awareness [11]. And, while in general information security awareness is acknowledged, the number of studies that consider it in depth is limited. This may be attributed to (a) the non-technical nature of security awareness [17] and / or (b) its scope, as it falls outside the traditional engineering and hard computer science domains [8]. Never the less, organizations with strong

technical security countermeasures, may still fail to protect their information systems. The human factor is considered the weakest link in the IS security chain [14].

In any given network in today's connected globe, the level of one user's IS security awareness may have a direct impact on the level of IS security exposure of all directly or indirectly connected users within that network. Information technology and the Internet have helped create non-collocated communities. Academic and research-based groupings form an important and influential component of these virtual collaborative research communities. However, despite the strategic nature of research (some of which subject to Intellectual Property Rights), there exist various levels of awareness about the security risk factor linked with virtual collaboration.

This study examines the IS security awareness levels of academics / researchers across different higher education institutions. The paper is structured into five sections. Following this introduction, the research methodology that underpins the research and relevant related work are summarized. Fieldwork results are then presented, followed by a discussion of the main findings. The paper concludes with key recommendations and directions for future research.

2 Methodology

The purpose of this study is to explore the levels of information systems security awareness of the virtual community of academic researchers who collaborate across different higher education institutions and environments.

The authors have used their own collaboration, extended to their institution and national academic environment, as the focus of this research. The first author used to be a member of staff of Zayed University in the UAE, prior to returning to the US as an academic member of Embry-Riddle Aeronautical University. The second author has during this period worked in two academic institutions in the UK, namely Salford University and Cardiff University. The focus of the research spans a duration of 4 years during which the two academics have collaborated across their respective institutions. Therefore, this study focuses on three academic environments in the UK, UAE, and the US and addresses the following main research question: *Are higher education research communities aware of the security challenges involved with virtual collaborative working that underpins academic research?*

An interpretive philosophical stance is adopted to conduct the research. The selected case study institutions not only exist in different environments, but also exhibit varying levels of security awareness and maturity while presenting some notable differences in their higher education vision, procedures and processes. To ensure consistency and validity of findings, multiple sources of data are gathered through the use of four main instruments: Interview, Questionnaire, Documentation, and Observation. The field work in Zayed University, Salford University, and Embry-Riddle University targeted research academics in different schools. This involved gathering 36 questionnaire responses and 10 interviews in the context of Zayed, 22 questionnaire responses and 10 interviews have been obtained in Salford, and 24 questionnaire responses and 8 interviews in Embry-Riddle University. Additional data was captured in the mode of direct observation [3] throughout the entire study. To measure the levels of users IS security awareness; the sources of data of this study

targeted the following 10 themes: (a) User's IS security awareness of available and accessible IS systems, and their intended use; (b) User's IS security awareness of existing IS security policies, standards, and guidelines; (c) User's IS security awareness of existing IS security laws and legislation; (d) User's IS security awareness of available IS staff and personnel; (e) User's IS security awareness of possible IS security threats and concerns; (f) User's IS security awareness of possible IS security solutions; (g) User's IS security awareness of available IS security training session and materials; (h) User's IS security awareness of available IS security documents and help material; (i) User's IS security awareness and perception of the value of university data; (j) User's IS security awareness and perception of their role in university's IS security. The chosen 10 themes were selected from a variety of prior IS security awareness studies [6], [9], [15], [16], and [17].

3 Related work

Information security awareness is concerned with creating and maintaining security-positive behavior [13]. According to the Information Security Forum [10], information security awareness can be defined as (a) the degree to which every user understands the importance of information security, (b) the appropriate level of information security to the organization, (c) users' security responsibility, and (d) users' behaviors and acts. Reference [17] defines information security awareness as the state where users in an organization are aware of, and ideally committed their security mission defined by the organization's end-user security guidelines. Information security awareness may cover a range of topics, including: password construction, password management, authentication, Internet usage, telephone fraud, physical e-mail usage and security, private information, virus protection and detection, PC security, software licensing, backups, building access, social engineering, identity theft and home office security [1].

The majority of today's IS attacks are not concerned with only circumventing the authentication process of an individual or an organization; they are more inclined to access confidential information. This has resulted in IS threats like phishing, identity theft, and social engineering [7]. While technical solutions are with no doubt necessary to address IS security problems, the consideration of humans, and more generally human factors, is equally important [1], [7]. The effective implementation and use of IS security awareness practices can lead to improved security for organizations. Reference [5] suggests that in order to avoid IS security breaches, organizations should provide users with IS security awareness training programs. The training program should cover areas like social engineering, password protection, and heightened physical security alertness. Reference [12] takes a step further by suggesting that organizations should implement a continuous security awareness training programs as part of the corporate asset protection program. But while information security is a key organizational goal and users have a responsibility to maintain this goal, it is important to understand that the implementation of an information security awareness program does not warrant that all users within the organization will understand their roles and responsibilities when it comes to information security [4]. Perhaps, this is why reference [16] recommends a

combination of measures to increase users IS security awareness. Reference [16] suggests that organizations use IS security awareness training, campaigning, and reward and punishment to establish an effective IS security awareness program. Reference [6] believes that Continuous reinforcement of proper IS security practices is needed to remind individuals of their role in information security. Both [1] and [13] recommend that a systematic approach to measure the effect of a security awareness program should be implemented to evaluate the contribution and the return on investment of such programs [13].

4 Field work

This section provides a summary of relevant fieldwork data across the three selected academic environments extended to their regional and national context. This is structured according to the above listed driving themes that underpin the research.

- **User's IS security awareness of available and accessible IS systems and their intended use:** The data evidence gathered for this category portrays that the examined institutions have a comparable IS infrastructure in terms of software, hardware, and network resources. The majority of academic researchers examined were aware of available IS resources. 87% of Zayed University respondents, 92% of University of Salford respondents, and 89% of Embry-Riddle University respondents referred to the availability of email, Internet, Intranet, extranet, IP telephony, wireless connectivity, course delivery, and administration applications, e-library system, and electronic databases. Most respondents were also aware of the intended use of these services.
- **User's IS security awareness of existing IS security policies, standards, and guidelines:** The examined institutions varied considerably in this category. Zayed University did not have any IS security policies, standards, or guidelines in place, while University of Salford and Embry-Riddle did. In terms of awareness, 74% of the respondents in Zayed University could not confirm the existence or the lack thereof of IS security policies, standards, and guidelines. Only 16% of the respondents in Zayed were able to confirm that no policies exist. 76% of the examined respondents in Salford, and 68% were able to reference existing universities' IS security policies, standard, and procedures.
- **User's IS security awareness of existing IS security laws and legislation:** In 2006, the UAE government issued two laws to combat electronic trading and cyber crimes. All respondents in Zayed University were not aware of existing IS legislation. 64% of the respondents in Salford referred to the Computer Misuse Act and the Data Protection Act. 90% of the users learned about the two acts through the Information Services Division, while the remaining 10% were informed through other resources. Similarly, 41% of the respondents in Embry-Riddle referenced the Data Protection Act and the Computer Misuse Act, the Digital Millennium Copy Right Act, and the Electronic Communication Privacy Act. 74% of the respondents were informed of many of these laws through the Information Technology Department web site.
- **User's IS security awareness of available IS staff and personnel:** 32% of

respondents in Zayed University were able to identify whom and how to contact in case of IT-security related problem or question. 65% of the respondents in Salford, and 76% of the respondents in Embry Riddle referred to the IT department web site for contact information of IT support staff. While the IT department in Zayed University maintained a web page for the university, it did not maintain a web page for the department with the exception of the hardware and software Help Desk.

- **User's IS security awareness of possible IS security threats and concerns:** Respondents in Salford and Embry-Riddle scored higher than their counterparts in Zayed in terms of awareness of IS security threats. 74% of IS users in Salford and 82% in Embry-Riddle respondents were able to identify several possible IS security threats including denial of service attack, social engineering, shoulder surfing, and email spam, compared to 41% in Zayed University. Many of which had an IS background.
- **User's IS security awareness of possible IS security solutions:** Respondents in Salford and Embry-Riddle University also scored higher than their counterparts in Zayed in terms of awareness of IS security solutions. 80% of IS users in Salford and 84% of respondents were familiar with security solutions such as data back up procedures, virus protection, and password change rules, compared to 46% of the respondents in Zayed University.
- **User's IS security awareness of available IS security training session and materials:** Although the Information Services Division in Zayed University offers periodical training session in Microsoft Office applications, it did not offer a single IS security training since the university inception in 1998. Naturally, none of the respondents were aware of any IS security training sessions. Respondents at Salford are required to attend an IS security training session as part of their orientation (Faculty, staff, and students). In addition to the mandatory session, the IS security coordinator offers periodical sessions throughout the academic year. In the Embry-Riddle University, IS security training is also part of the induction program for both faculty and students. Training materials are also available online.
- **User's IS security awareness of available IS security documents and help material:** Similar to the training category, respondents in Zayed University were not aware of IS security documents and help material mainly due to non-availability. 54% of the respondents at Salford, and 67% of respondents at Embry-Riddle University were able to locate key IS security documents and help materials.
- **User's IS security awareness and perception of the value of university data:** 46% of the respondents in Zayed University viewed university data as valuable and worthy of protection, while 54% viewed the university data as "of no interest to hackers". Many of these came from academics with less computer/IS background. 96% of the respondents in the University of Salford, and 88% Embry-Riddle University viewed university data as valuable, private, confidential, and worthy of protection.
- **User's IS security awareness and perception of his/her role in university's IS security:** In this last category, 88% of the respondents in Zayed University believed that they have a role in IS security, 65% of which could not define it.

They also believed that the full responsibility of IS security falls on the shoulder of the Information Service Division. Surprisingly, many of these are IS users who had some sort of IS background, tend to take for granted and fully trust their institution in implementing security policies. On the other hand, the remaining 13%, was mainly academics from computer science and information technology disciplines who viewed their role as "first line of defense" to university IS security. 96% of the respondents in the UK university of Salford, and 86% of respondents from Embry Riddle viewed their role in the overall IS security cycle as important. More than 70% in both cases viewed the protection of their PC password and data as the main goals.

5 Discussion

The findings of this study indicate a considerable difference between the level of IS security awareness of academic researchers in the UAE and those of academic researchers in the UK and the US. The level of IS security awareness of academic researchers in each environment correlated with the level of IS security awareness supporting tools utilized in that environment as shown in table (1) and figure (1). Respondents in the University of Salford and Embry-Riddle University appeared more aware of IS security-related matters than their counter parts in Zayed University. The higher level of IS security awareness in the case of the UK and the US can mainly be attributed to the existence of IS security awareness supporting tools and activities. The IS security function in the examined institutions in the UK and the US appeared more supported, coordinated, regulated, and centralized than that in the UAE. The majority of academic researchers in Zayed University were not aware of possible IS security threats and their role in defending against them. They were not aware of whom to reach in case of an IS security problem, and they were not aware of proper policies, standards, and guidelines that should govern their access and use of IS systems. It should be noted that (a) Academics from areas other than computer science and information systems exhibited a lower level of security awareness than academics with a computing background, (b) users with a computer science background tend to take for granted and fully trust their institution in implementing security policies which may result in overlooking basic security threats, and (c) academics tend to work from home, or while on the move (including conference venues, hotels, etc…) which makes them prone to wireless network security threats.

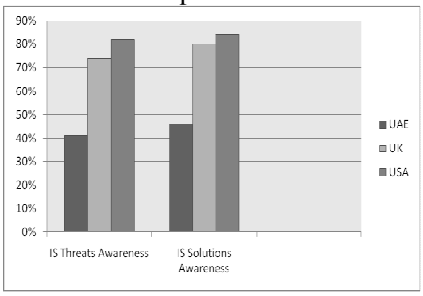

Fig. 1 User's IS Security Awareness

Table 1 – Used IS Security Tools

Case Study	IS Security Policies	IS security Training	IS security Documentation
UAE	X	X	X
UK	√	√	√
USA	√	√	√

The low-perceived value of IS security and the data stored by the examined institution in the UAE is a natural result of the lack of emphasis shown by the university management; which is visible through: (a) Lack of IS security training, (b) Lack of IS security policies, (c) Lack of IS security coordination. Inversely, the higher level of IS security awareness in the examined institutions in the UK and the US can be attributed to the university emphasis and commitment to IS security awareness, by: (a) Establishment, communication, and enforcement of IS security training programs, (b) Establishment, communication, and enforcement of IS security policies; (c) Establishment of a coordinated IS security function. While understanding that no single practice described will work everywhere, from the findings of this study, and in correlation with [14] and [16], the authors believe that the following steps have the potential to increase the level of IS security awareness, and consequently the level of IS security awareness in UAE and more generally academic institutions in developing economies: (a) Establishment and communication of IS security policies and procedures to academic members of staff; (b) Campaign and advertise IS security awareness best practices and IS security training sessions and materials; (c) Train academic members on IS security best practices to increase their awareness; (d) Reward secure academic collaborations and identify / disseminate ill security practices; and (e) Conduct continuous evaluation and readjustment.

6 Conclusion

The paper explores if higher education research communities are aware of the security challenges related to the virtual collaborative working that underpins academic research. The examined institutions are believed to be a typical representation of higher education institutions within the selected communities.

The findings of this study indicate that although the examined institutions presented a similar IS infrastructure, and employed similar IS security technical measures, the level of IS security awareness varied considerably. This variance can be directly attributed to the level of IS security awareness supporting tools and activities utilized by the institution. The study indicates that the level of IS security awareness correlated with the availability and enforcement of IS security awareness supporting tools such as training, policies, documents, and coordination. The low level of IS security awareness of academic researchers in the case of the UAE, and more generally academic institutions from developing countries, constitute a higher level of possible risk of IS security threats to other academic researchers from developed countries who undertake joint collaborative research. Developing countries tend to have a large underground market for illegal software [18] and an increased number of unaware users who can easily become easy targets to criminals and hackers.

The main research question that underpins the paper deserves further and more in-depth exploration using larger samples of academic users across institutions, while using larger collaborative academic networks or communities as case studies. This constitutes ongoing research to be reported by the authors in future publications.

6 References

[1] Rezgui, Y., Marks, A.: Information security awareness in higher education: An exploratory study, Computers and Security, 27 (7-8) (2008).
[2] Updegrove, D., Gordon, W.: Computers and Network Security in Higher Education", EDUCAUSE, (2003).
[3] Yin, R.K.: Applications of case study research, London, SAGE. (2003).
[4] Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Computers & Security., (2009).
[5] Bray, T.J: Security actions during reduction in workforce efforts: what to do when downsizing. Information systems security. (2002).
[6] Cooper, M.: Information Security Training- Lessons Learned Along the Trail. Proceedings of the 36th annual ACM SIGUCCS conference on User services conference, (2009).
[7] Dlimini, M., Eloff, j., Eloff, M.: Information security: The moving target". Computers & Security, (2008).
[8] Dunlop, C., Kling, R.: Social Relationship in Electronic Commerce. Introduction in Computerization and Controversy- Value Conflicts and Social change, (ed. C. Dunlop and R. Kling). Academic Press, New York, USA, (1992).
[9] EDUCAUSE: Center for Applied Research: Information Technology Security: "Governance, strategy, and practice in Higher Education". (2003).
[10] ISF- International Security Forum. The Forum's Standard of Good Practice for IS security. Cited May 18th 2006 from http://www.isfsecuritystandard.com/index_ie.htm.
[11] Katz, F.H.: The Effect of a University Information Security Survey on Instructing Methods in Information Security. In: Proceedings of the 2nd annual conference on Information security curriculum development, (2005).
[12] Kovacich, G.: Information system security Officer's Guide: Establishing and Managing an Information Protection Program. USA: Butterworth-Heinemann, (1998).
[13] Kruger, H.A., Kearney, W.D.: A prototype for assessing information security awareness. Computers & Security, 25:1, pp. 289-296, (2006).
[14] Mitnick, K.D., Simon, W.L.: The Art of Deception: Controlling the Human Element of Security, Indianapolis, IN: Wiley, (2002)
[15] North, M., Roy, G., North, S.: Computer Security Ethics Awareness in University Environments: A Challenge for Management of Information Systems, (2006).
[16] Puhakainen, P.: A Design Theory for Information Security Awareness., (2006).
[17] Siponen, M.T.: A Conceptual Foundation for Organizational Information Security awareness. Information Management & Computer Security, (2000).
[18] Joseph, M.: IT in the Middle East: Overview. Proceedings of the 7th conference on Information technology education, (2006).